CLAIMS

1. A computing device comprising:

a processing system;

a memory coupled to said processing system;

a system program stored in said memory;

a secure checking program for repeatedly authenticating said system program during operation of the computing device to ensure that the system program is not modified during execution.

2. The computing device of claim 1 and further comprising a digital certificate associated with said system program, wherein said digital certificate includes information defining a secure state of the system program.

3. The computing device of claim 2 wherein said information includes a hash of the system program.

4. The computing device of claim 3 wherein said hash is asymmetrically encrypted using a private key to produce a signature associated with the system program.

5. The computing device of claim 4 wherein said information includes a public key associated with said private key.

6. The computing device of claim 5 wherein the secure checking program authenticates the system program by:

decrypting said signature using said public key to produce a decrypted signature; and

comparing a hash of a current state of the system program with said decrypted signature.

7. The computing device of claim 2 wherein said information is asymmetrically encrypted using a private key belonging to a manufacturer of said computing device.

8. The computing device of claim 2 wherein said information includes a die identification number uniquely associated with the computing device.

9. The computing device of claim 8 wherein said secure checking program compare the die identification number stored in the certificate with a die identification number stored in the computing device.

10. The computing device of claim 2 wherein the secure checking program can disable functions of the computing device if a modification of the system program or a modification of the certificate is detected.

11. A method of controlling the operation of a computing device, comprising the step of:

comparing a current state of a system program executed by the computing device with a known secure state of the system program;

repeating the comparing step during operation of the computing device to determine any variation of the system program from the known secure state.

12. The method of claim 11 wherein said comparing step comprises the step of comparing information in a digital certificate associated with the system program to said current state to determine if a modification of the system program has occurred.

13. The method of claim 12 and wherein the comparing step further comprising the step of authenticating a firmware certificate field of the digital certificate, where the firmware certificate field contains an encrypted hash of selected fields of the digital certificate.

14. The method of claim 13 wherein said authenticating step comprises the step of asymmetrically decrypting the hash using a public key to produce a signature associated with the digital certificate.

15. The method of claim 14 wherein said public key is stored in the digital certificate.

16. The method of claim 15 wherein said authenticating step further comprises the step of comparing a hash of a current state of the system program with said signature.

17. The method of claim 12 wherein said comparing step comprises the step of authenticating an originator's public key stored in the digital certificate, where the originator's public key is associated with a firmware originator.

18. The method of claim 17 wherein said authenticating step comprises the steps of:

decrypting a signature associated with originator's public key with reference to a manufacturer's public key, where the manufacturer's public key is associated with a manufacturer of the computing device, to produce a decrypted signature;

generating a hash of the originator's public key and

comparing the decrypted signature with the hash.

19. The method of claim 17 and wherein the comparing step further comprises the step of authenticating the system firmware.

20. The method of claim 19 wherein the step of authenticating the system firmware comprises the steps of:

decrypting an encrypted hash of an initial state of the system firmware to produce a signature for the initial state;

generating a hash of a current state of the system firmware; and

comparing the signature to the hash.

21. The method of claim 12 wherein said comparing step comprises the step of determining the validity of a die identification number stored in the digital certificate by comparing the die identification number stored in the certificate with a die identification number stored in the computing device.

22. The method of claim 12 and further comprising the step of disabling functions of the computing device if a modification of the system firmware or a modification of the certificate is detected.

23. The method of claim 11 wherein said repeating step comprises the step of repeating said comparing step during periods of inactivity in the computing device.

24. The method of claim 11 wherein said repeating step comprises the step of repeating said comparing step when initiated by a software application.